CVE-2018-5223

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-5223
State	PUBLIC
Assigner	security@atlassian.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-29 13:29:00 UTC
Updated	2018-04-24 12:54:00 UTC
Description	Fisheye and Crucible did not correctly check if a configured Mercurial repository URI contained values that the Windows op

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Crucible	All	All	All	All
Application	Atlassian	Crucible	All	All	All	All
Application	Atlassian	Fisheye	All	All	All	All
Application	Atlassian	Fisheye	All	All	All	All

References

Reference
[CRUC-8181] Argument injection through Mercurial repository uri handling on Windows - CVE-2018-5223 - Create and track feature requests
[FE-7014] Argument injection through Mercurial repository uri handling on Windows - CVE-2018-5223 - Create and track feature requests for A
Atlassian FishEye and Crucible CVE-2018-5223 Remote Code Execution Vulnerability
Page Not Found - Atlassian Documentation
Fisheye and Crucible Security Advisory 2018-03-28 | Crucible Server 4.8 | Atlassian Documentation
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**